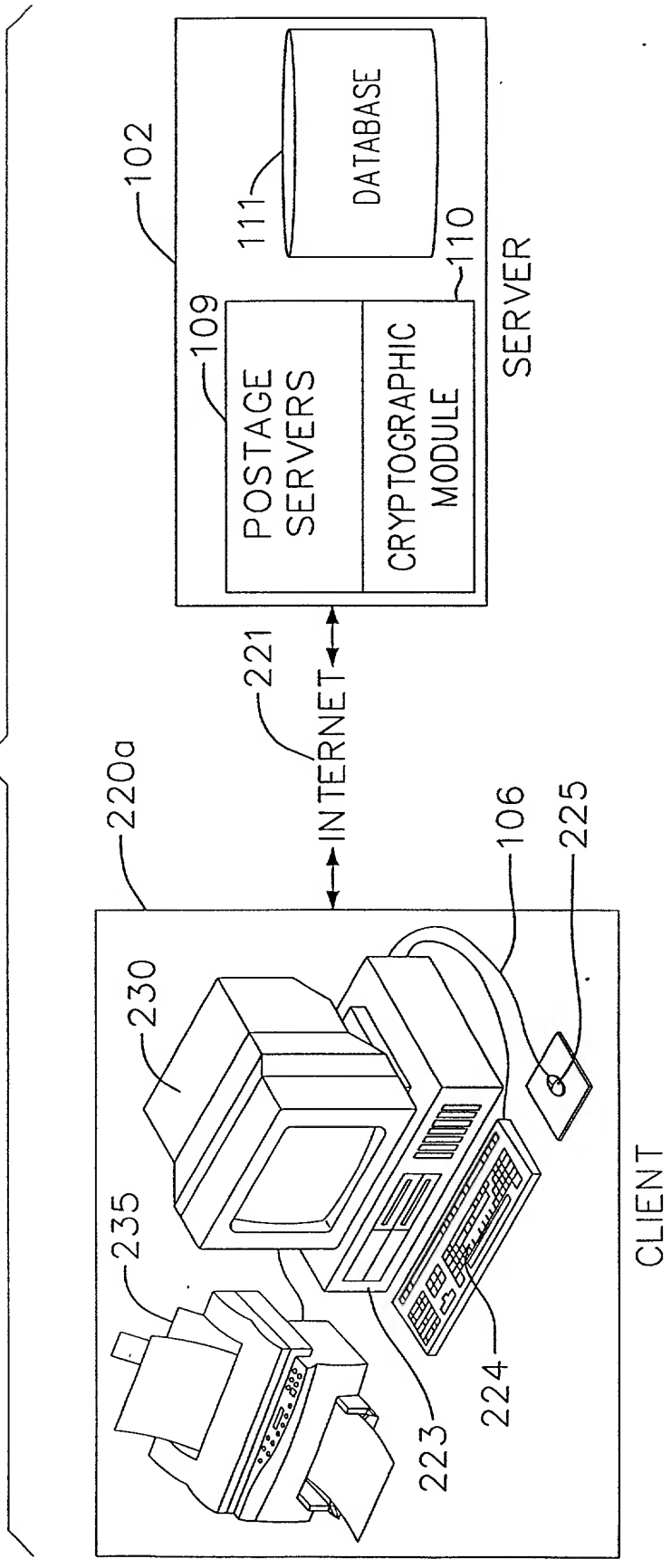
FIG. 1


102
111
DATABASE
110
109
POSTAGE SERVERS
CRYPTOGRAPHIC MODULE
SERVER
221
INTERNET
220a
106
225
230
235
223
224
CLIENT

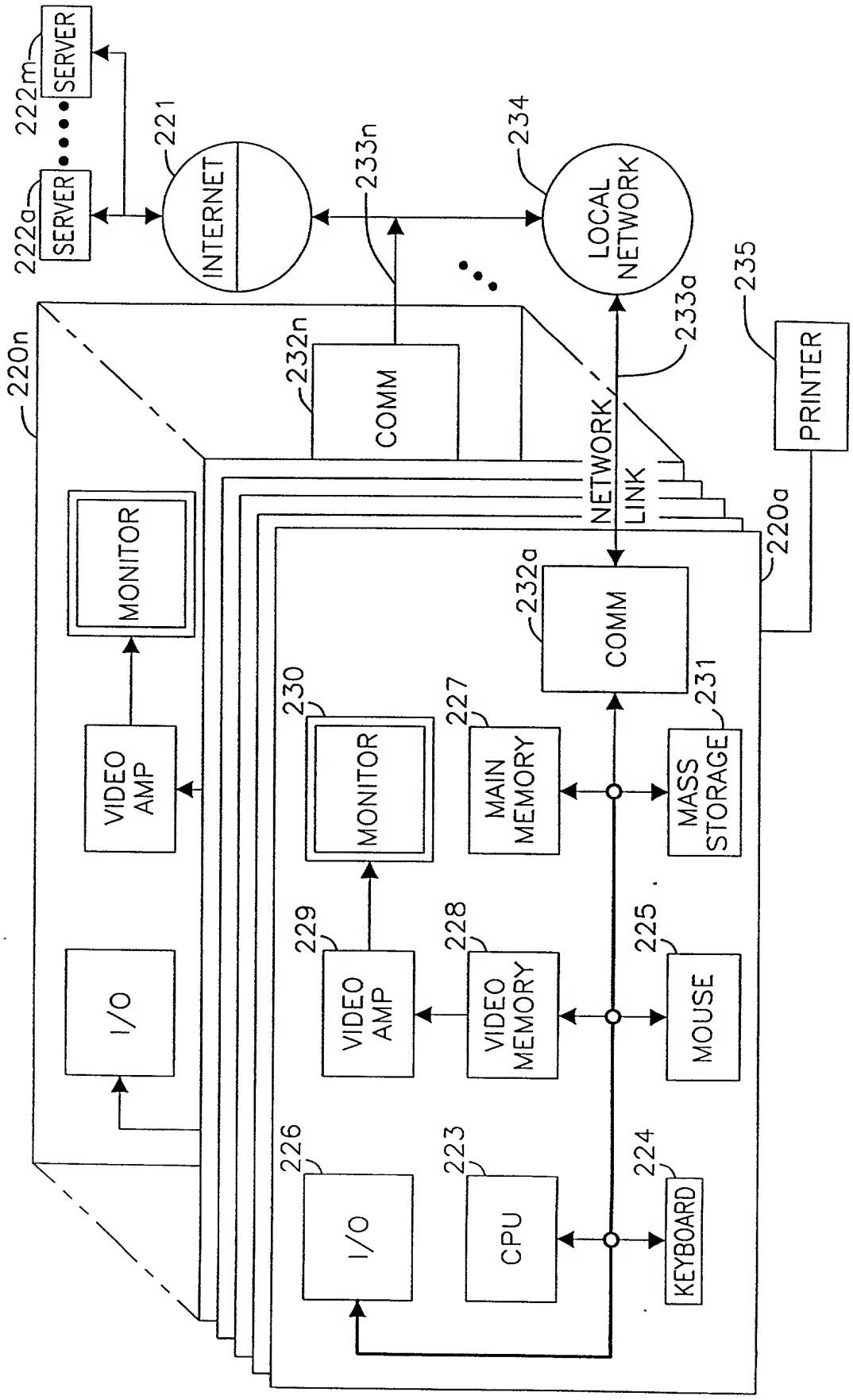
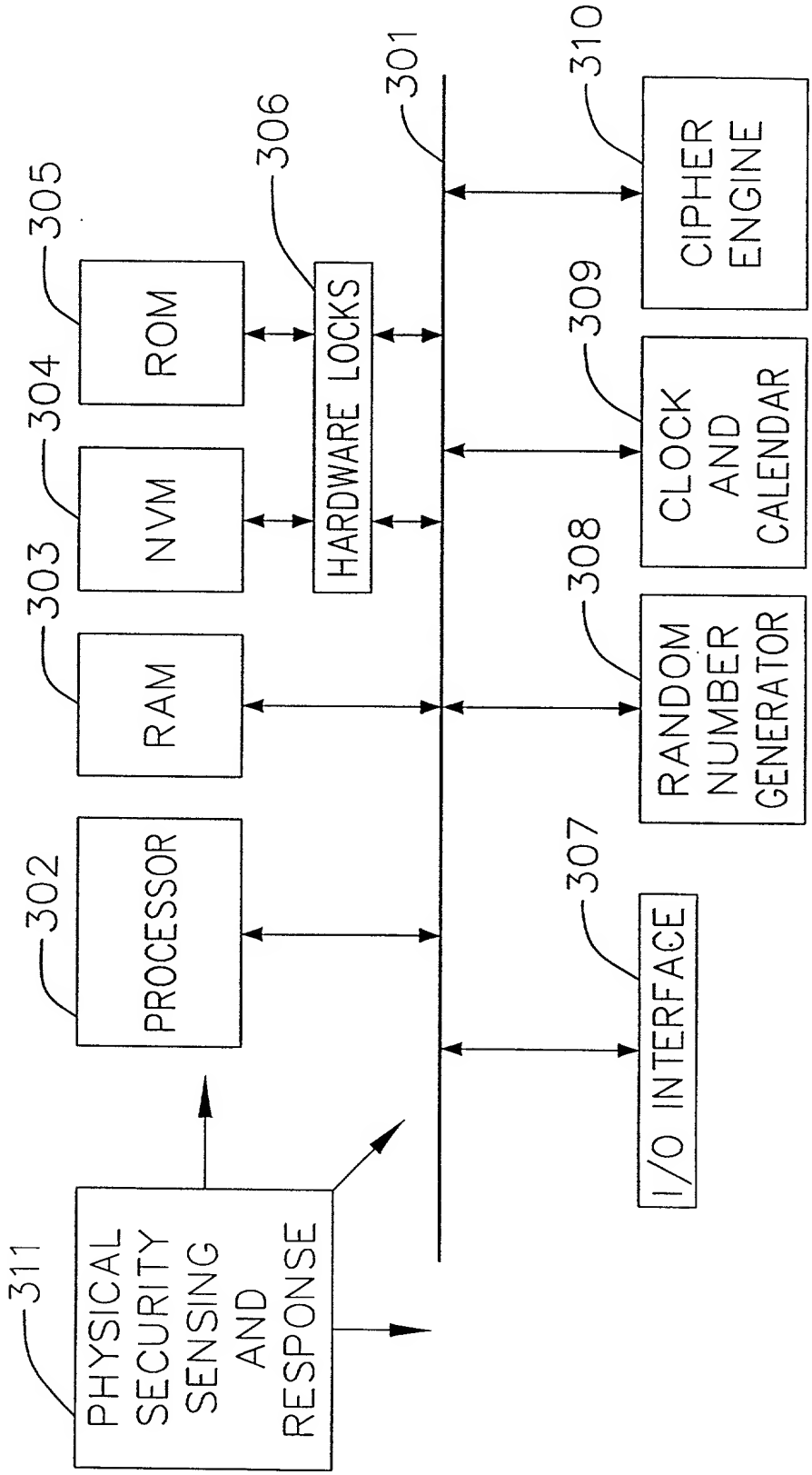

222m
SERVER
222a
SERVER
221
INTERNET
233n
234
LOCAL NETWORK
235
PRINTER
220n
232n
COMM
233a
NETWORK LINK
220a
MONITOR
232a
COMM
230
MONITOR
227
MAIN MEMORY
231
MASS STORAGE
VIDEO AMP
229
VIDEO AMP
228
VIDEO MEMORY
225
MOUSE
I/O
226
I/O
223
CPU
224
KEYBOARD

FIG. 2

FIG. 3


301
302
PROCESSOR
303
RAM
304
NVM
305
ROM
306
HARDWARE LOCKS
307
I/O INTERFACE
308
RANDOM NUMBER GENERATOR
309
CLOCK AND CALENDAR
310
CIPHER ENGINE
311
PHYSICAL SECURITY SENSING AND RESPONSE

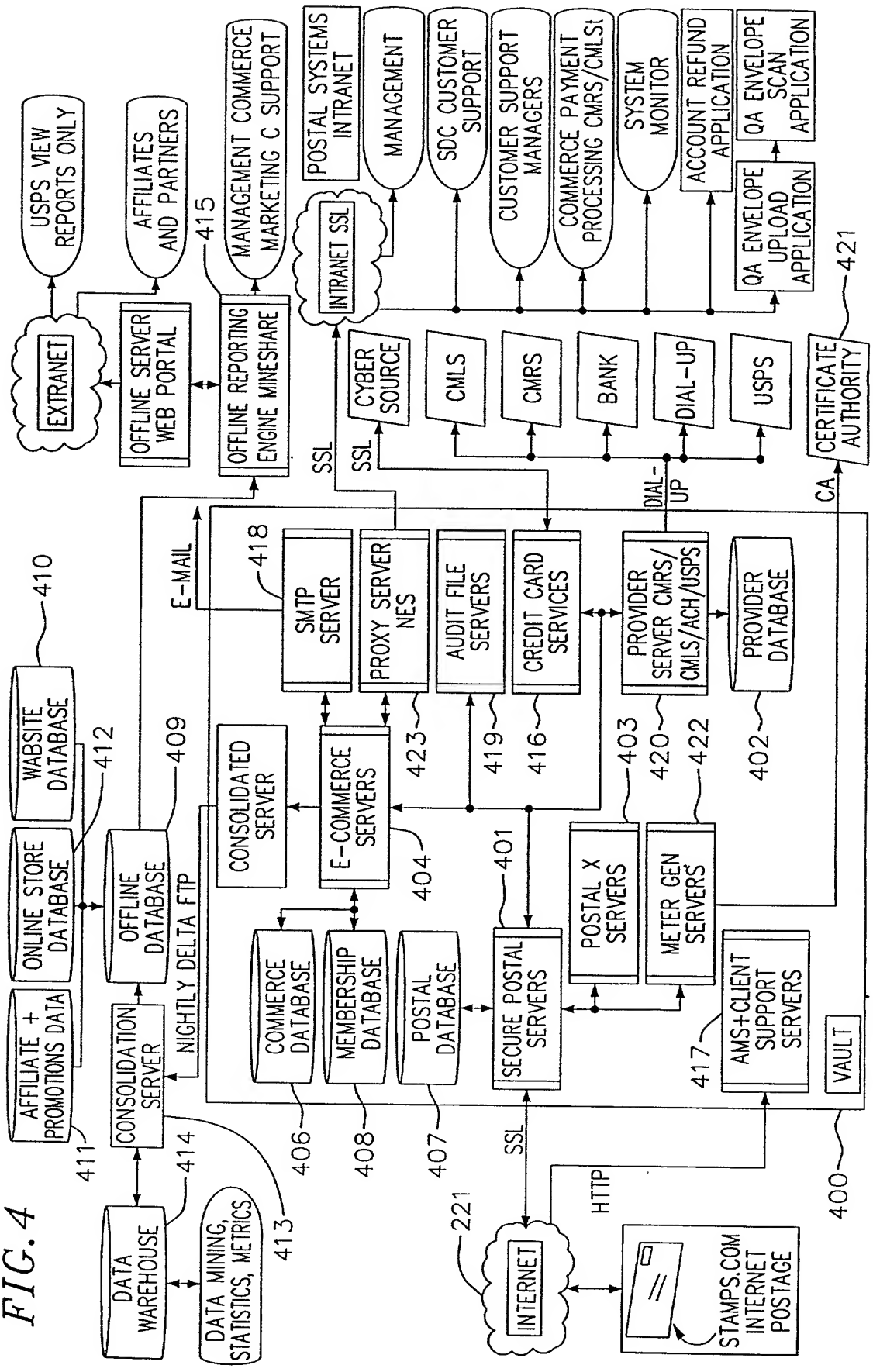

USPS VIEW REPORTS ONLY
AFFILIATES AND PARTNERS
MANAGEMENT COMMERCE MARKETING C SUPPORT
415
POSTAL SYSTEMS INTRANET
MANAGEMENT
SDC CUSTOMER SUPPORT
CUSTOMER SUPPORT MANAGERS
COMMERCE PAYMENT PROCESSING CMRS/CMLS
SYSTEM MONITOR
ACCOUNT REFUND APPLICATION
QA ENVELOPE SCAN APPLICATION
QA ENVELOPE UPLOAD APPLICATION
421
EXTRANET
OFFLINE SERVER WEB PORTAL
OFFLINE REPORTING ENGINE MINESHARE
INTRANET SSL
CYBER SOURCE
CMLS
CMRS
BANK
DIAL-UP
USPS
CERTIFICATE AUTHORITY
SSL
SSL
DIAL-UP
CA
E-MAIL
418
SMTP SERVER
PROXY SERVER NES
AUDIT FILE SERVERS
CREDIT CARD SERVICES
PROVIDER SERVER CMRS/CMLS/ACH/USPS
PROVIDER DATABASE
410
WABSITE DATABASE
412
409
CONSOLIDATED SERVER
423
419
416
403
420
422
402
ONLINE STORE DATABASE
OFFLINE DATABASE
NIGHTLY DELTA FTP
E-COMMERCE SERVERS
404
401
POSTAL X SERVERS
METER GEN SERVERS
AFFILIATE + PROMOTIONS DATA
CONSOLIDATION SERVER
COMMERCE DATABASE
MEMBERSHIP DATABASE
POSTAL DATABASE
SECURE POSTAL SERVERS
AMS+CLIENT SUPPORT SERVERS
VAULT
417
411
414
406
408
407
SSL
413
DATA WAREHOUSE
DATA MINING, STATISTICS, METRICS
221
INTERNET
HTTP
STAMPS.COM INTERNET POSTAGE
400

FIG. 4

FIG. 5

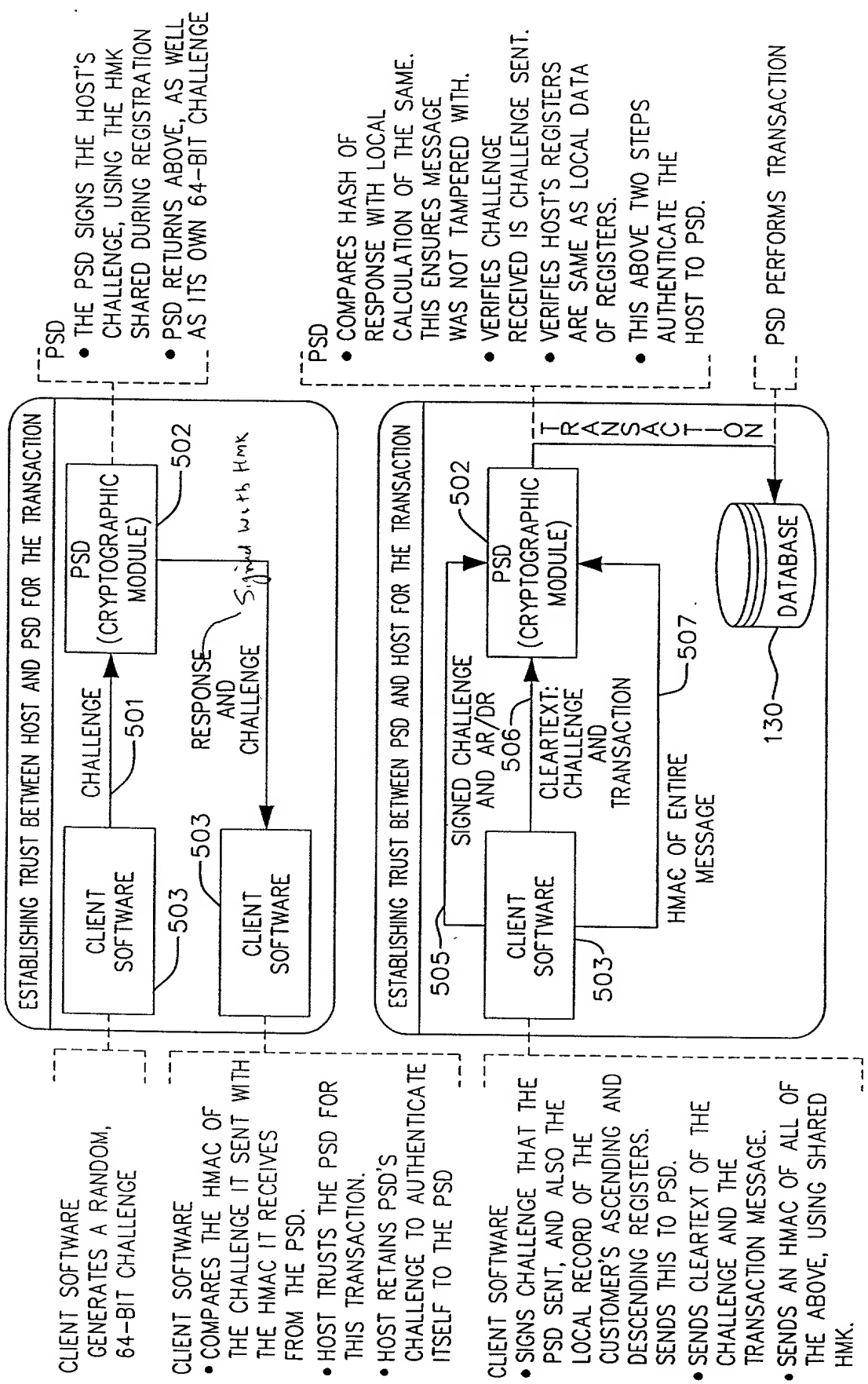
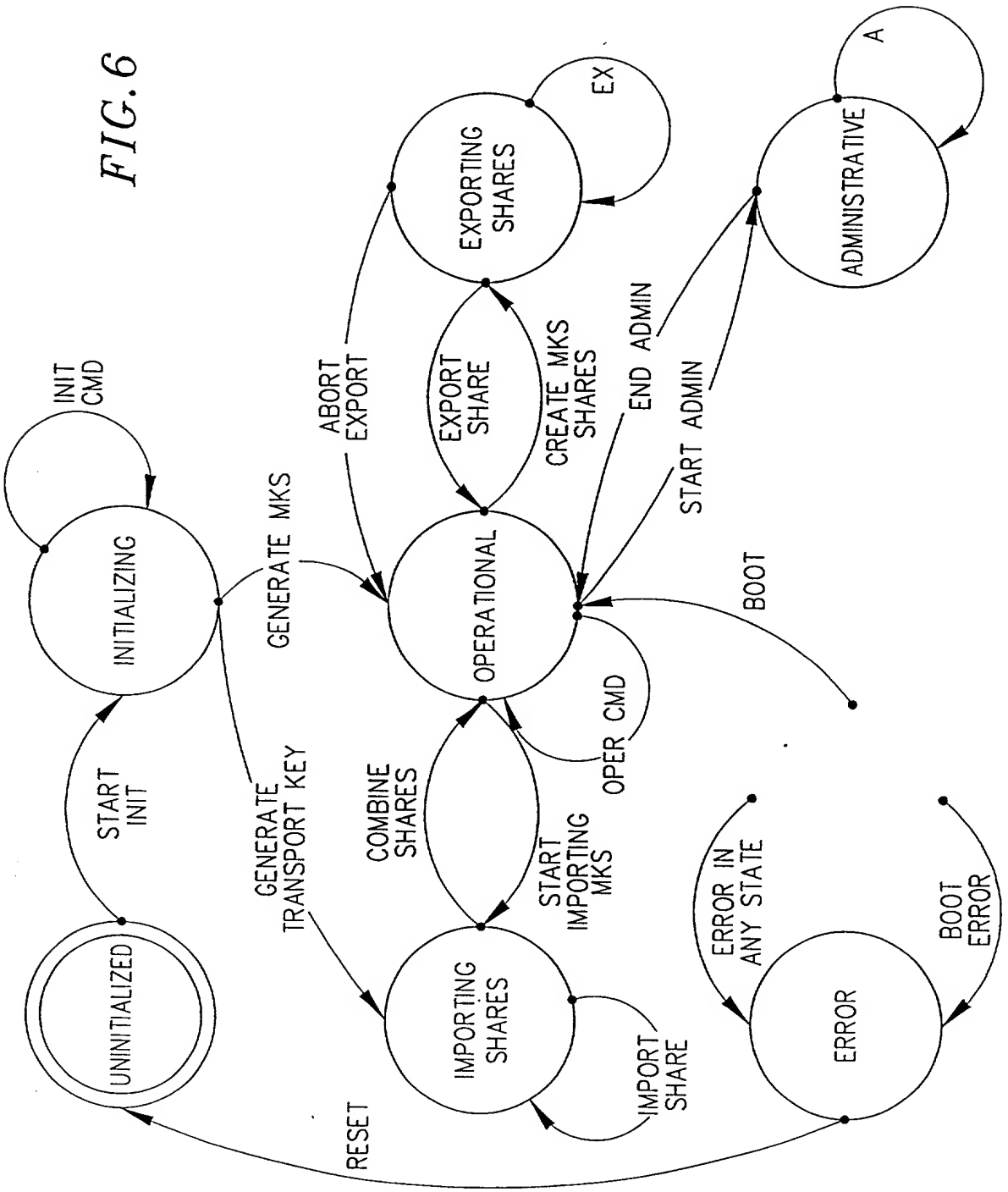

ESTABLISHING TRUST BETWEEN HOST AND PSD FOR THE TRANSACTION
CLIENT SOFTWARE
CHALLENGE
501
PSD (CRYPTOGRAPHIC MODULE)
502
503
RESPONSE AND CHALLENGE
Signed with HMK
CLIENT SOFTWARE
503
CLIENT SOFTWARE GENERATES A RANDOM, 64-BIT CHALLENGE
CLIENT SOFTWARE
• COMPARES THE HMAC OF THE CHALLENGE IT SENT WITH THE HMAC IT RECEIVES FROM THE PSD.
• HOST TRUSTS THE PSD FOR THIS TRANSACTION.
• HOST RETAINS PSD'S CHALLENGE TO AUTHENTICATE ITSELF TO THE PSD
PSD
• THE PSD SIGNS THE HOST'S CHALLENGE, USING THE HMK SHARED DURING REGISTRATION
• PSD RETURNS ABOVE, AS WELL AS ITS OWN 64-BIT CHALLENGE
ESTABLISHING TRUST BETWEEN PSD AND HOST FOR THE TRANSACTION
505
SIGNED CHALLENGE AND AR/DR
506
502
PSD (CRYPTOGRAPHIC MODULE)
CLIENT SOFTWARE
503
CLEARTEXT: CHALLENGE AND TRANSACTION
HMAC OF ENTIRE MESSAGE
507
130
DATABASE
TRANSACTION
CLIENT SOFTWARE
• SIGNS CHALLENGE THAT THE PSD SENT, AND ALSO THE LOCAL RECORD OF THE CUSTOMER'S ASCENDING AND DESCENDING REGISTERS. SENDS THIS TO PSD.
• SENDS CLEARTEXT OF THE CHALLENGE AND THE TRANSACTION MESSAGE.
• SENDS AN HMAC OF ALL OF THE ABOVE, USING SHARED HMK.
PSD
• COMPARES HASH OF RESPONSE WITH LOCAL CALCULATION OF THE SAME. THIS ENSURES MESSAGE WAS NOT TAMPERED WITH.
• VERIFIES CHALLENGE RECEIVED IS CHALLENGE SENT.
• VERIFIES HOST'S REGISTERS ARE SAME AS LOCAL DATA OF REGISTERS.
• THIS ABOVE TWO STEPS AUTHENTICATE THE HOST TO PSD.
PSD PERFORMS TRANSACTION

FIG. 6


UNINITIALIZED
INITIALIZING
OPERATIONAL
EXPORTING SHARES
ADMINISTRATIVE
IMPORTING SHARES
ERROR
INIT CMD
START INIT
GENERATE MKS
GENERATE TRANSPORT KEY
ABORT EXPORT
EXPORT SHARE
CREATE MKS SHARES
EX
END ADMIN
START ADMIN
A
BOOT
OPER CMD
COMBINE SHARES
START IMPORTING MKS
IMPORT SHARE
ERROR IN ANY STATE
BOOT ERROR
RESET

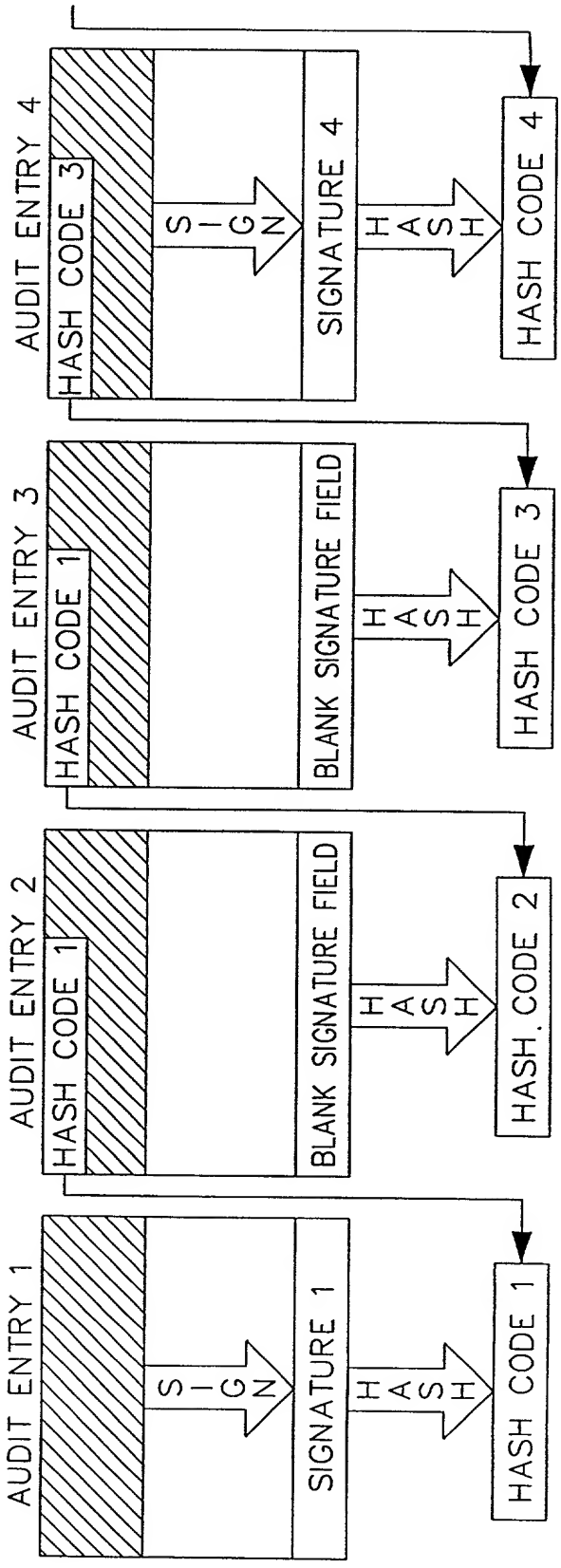

AUDIT ENTRY 1
SIGN
SIGNATURE 1
HASH
HASH CODE 1
AUDIT ENTRY 2
HASH CODE 1
BLANK SIGNATURE FIELD
HASH
HASH CODE 2
AUDIT ENTRY 3
HASH CODE 1
BLANK SIGNATURE FIELD
HASH
HASH CODE 3
AUDIT ENTRY 4
HASH CODE 3
SIGN
SIGNATURE 4
HASH
HASH CODE 4

FIG. 7

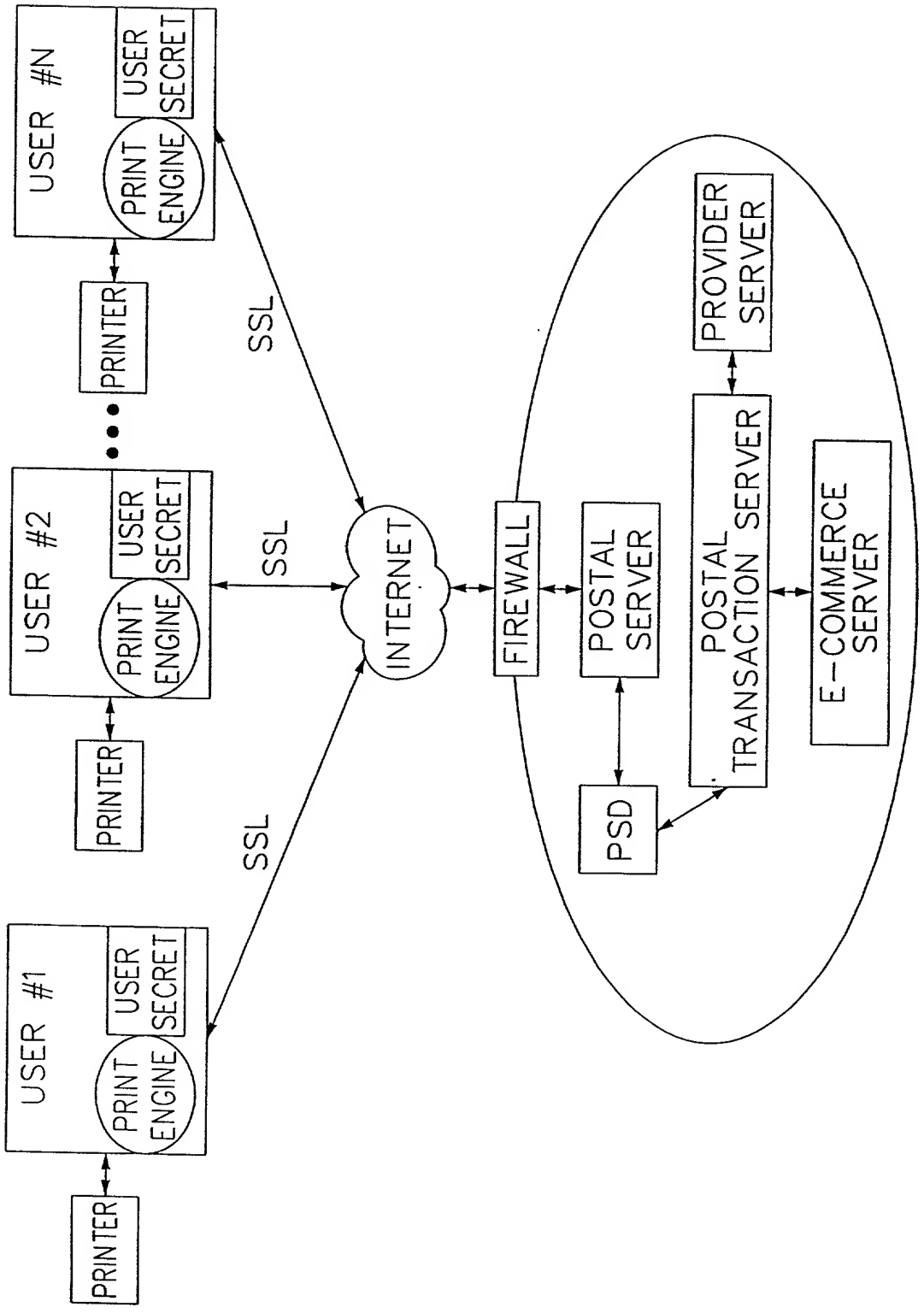

USER #N
USER SECRET
PRINT ENGINE
PRINTER
USER #2
USER SECRET
PRINT ENGINE
PRINTER
USER #1
USER SECRET
PRINT ENGINE
PRINTER
SSL
SSL
SSL
INTERNET
FIREWALL
POSTAL SERVER
PSD
PROVIDER SERVER
POSTAL TRANSACTION SERVER
E-COMMERCE SERVER

FIG. 8

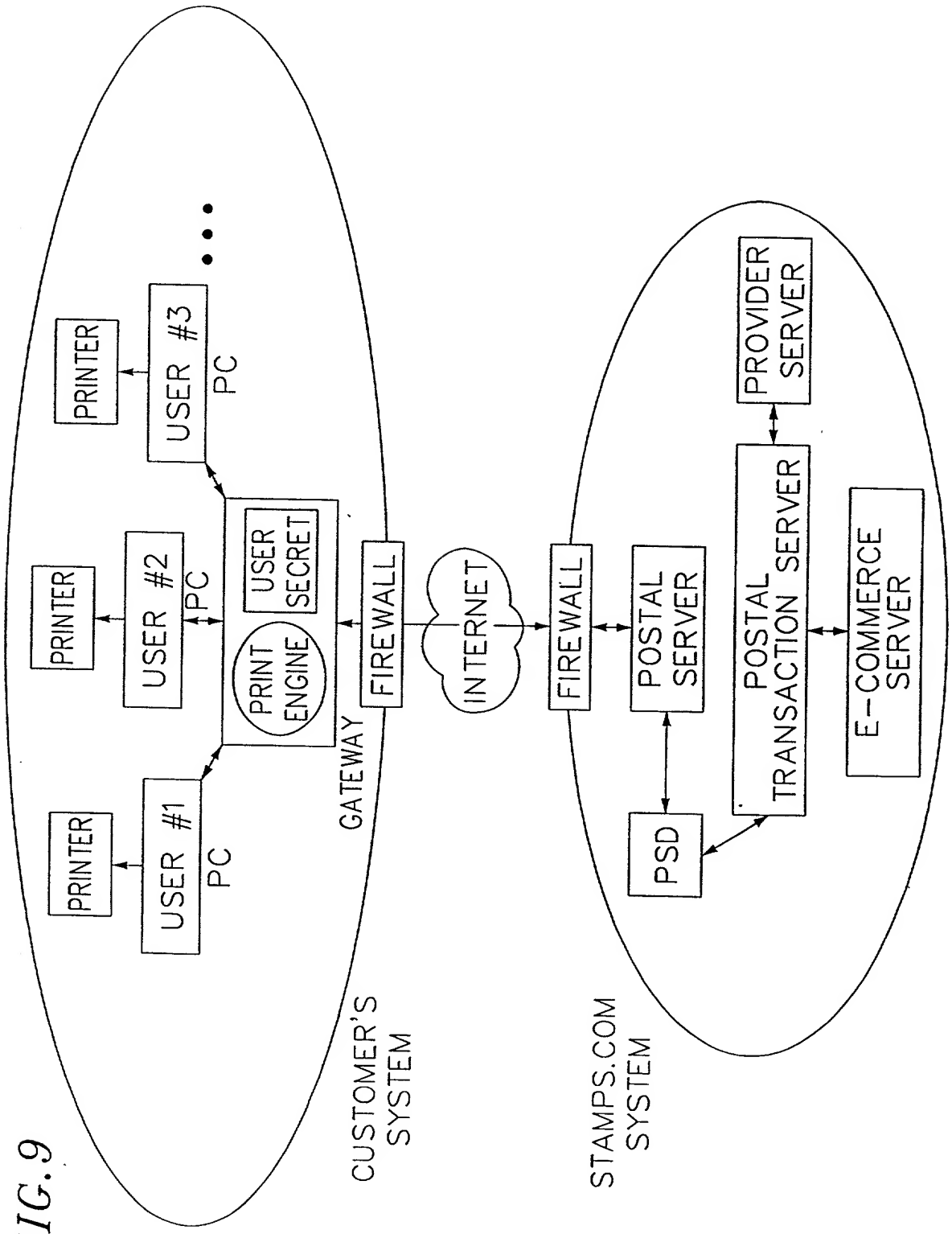
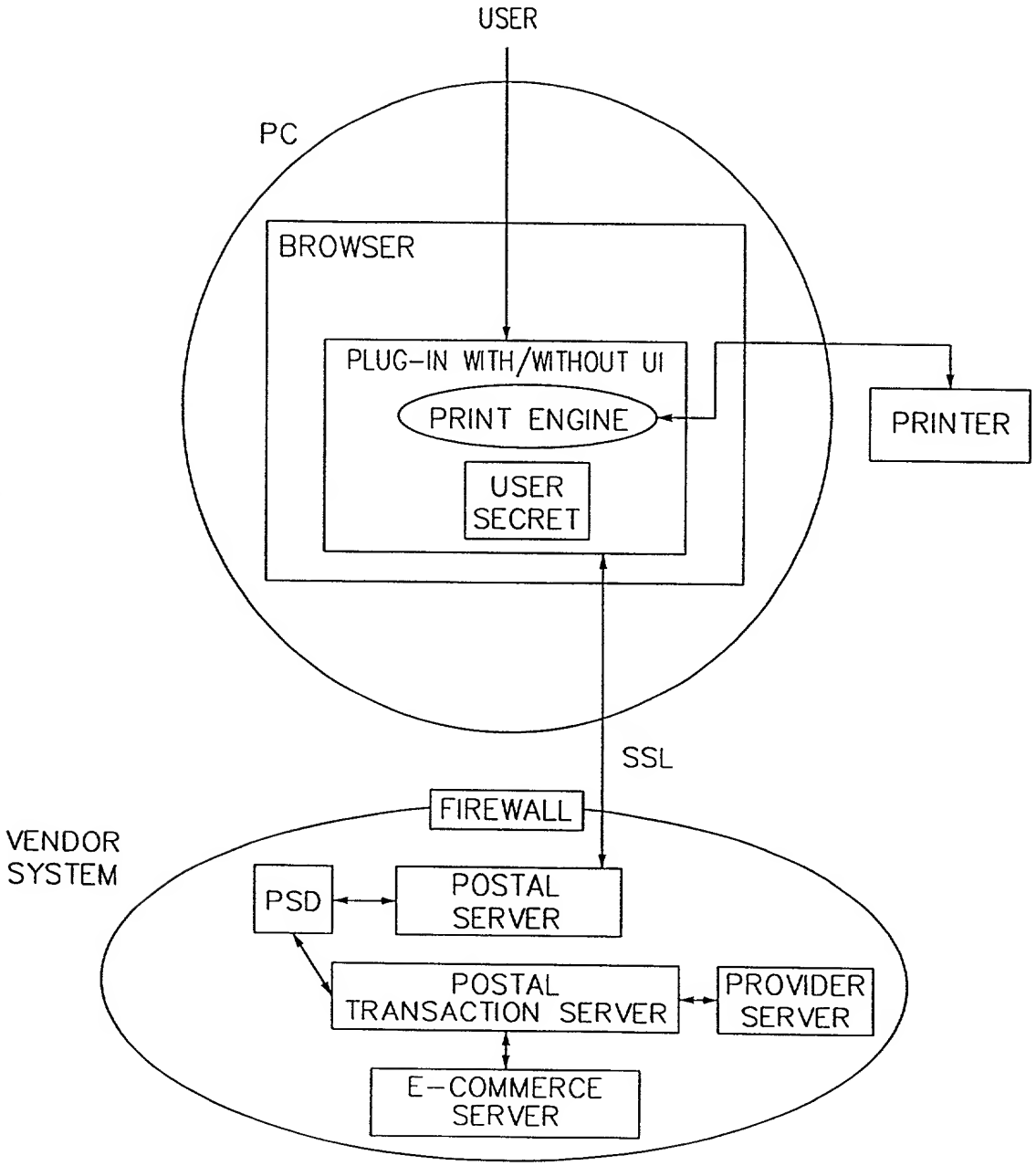

CUSTOMER'S SYSTEM
PRINTER
USER #1
PC
PRINTER
USER #2
PC
PRINTER
USER #3
PC
PRINT ENGINE
USER SECRET
GATEWAY
FIREWALL
INTERNET
FIREWALL
POSTAL SERVER
PSD
POSTAL TRANSACTION SERVER
PROVIDER SERVER
E-COMMERCE SERVER
STAMPS.COM SYSTEM

FIG. 9

FIG. 10


USER
PC
BROWSER
PLUG-IN WITH/WITHOUT UI
PRINT ENGINE
USER SECRET
PRINTER
SSL
FIREWALL
VENDOR SYSTEM
PSD
POSTAL SERVER
POSTAL TRANSACTION SERVER
PROVIDER SERVER
E-COMMERCE SERVER